

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-304293

(43)Date of publication of application : 24.10.2003

(51)Int.Cl.

H04L 12/66

(21)Application number : 2002-107281

(71)Applicant : HITACHI LTD

(22)Date of filing : 10.04.2002

(72)Inventor : MURAKAMI TOSHIHIKO

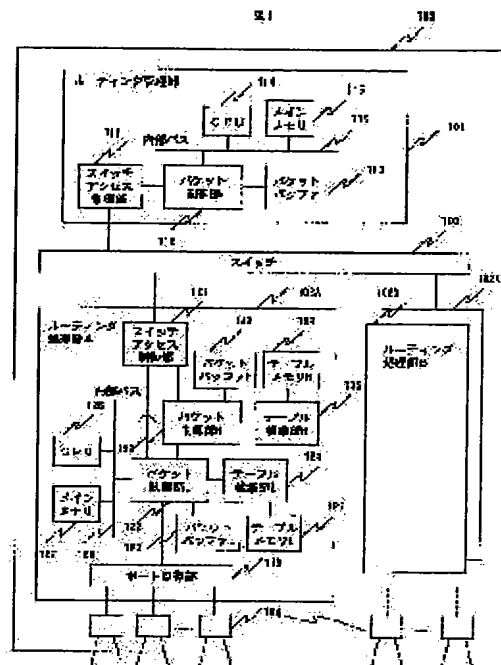
(54) PACKET REPEATER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method allowing high-speed packet processing even if the high-layer packet processing is performed in a packet repeater, such as a router, a layer 2-3 switch.

SOLUTION: In the packet repeater, such as the router, the layer 2-3 switch, the multilayer high-speed packet processing method is applied to a packet which is decided to perform relay by layer 2 and 3 routing and low-layer packet filtering by means of a conventional ASIC (Application-Specific Integrated Circuit).

Additionally, packet repeating processing is performed by preparing a plurality of high-layer filtering functions by means of the ASIC or a network processor according to the analyzing contents of every layer or the packet.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-304293

(P2003-304293A)

(43) 公開日 平成15年10月24日 (2003. 10. 24)

(51) Int.Cl.⁷

H 0 4 L 12/66

識別記号

F I

H 0 4 L 12/66

テマコード^{*}(参考)

B 5 K 0 3 0

審査請求 未請求 請求項の数 7 O L (全 11 頁)

(21) 出願番号 特願2002-107281(P2002-107281)

(22) 出願日 平成14年4月10日 (2002. 4. 10)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 村上 俊彦

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74) 代理人 100075096

弁理士 作田 康夫

Fターム(参考) 5K030 GA03 GA15 HA08 HD03 HD05

KA05 KA15 KX24 LB05 LC15

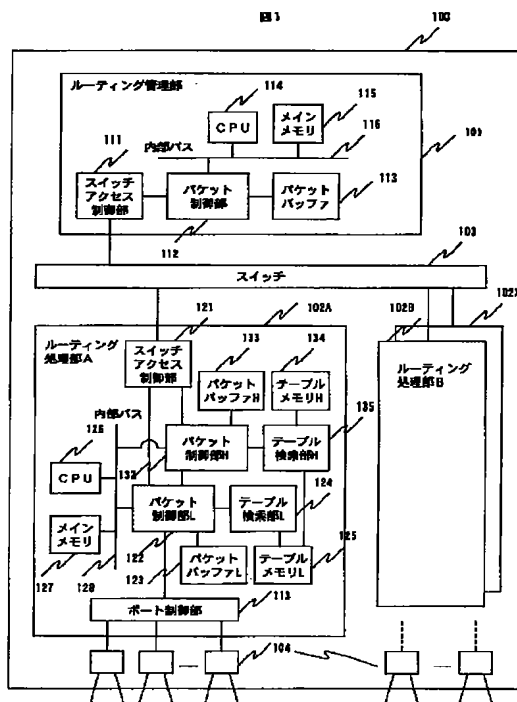
LD19 LE09 MD08

(54) 【発明の名称】 パケット中継装置

(57) 【要約】

【課題】 ルータやレイヤ2-3スイッチのようなパケット中継装置において、高レイヤのパケット処理を行う場合でも高速なパケット処理ができる方法を提供する。

【解決手段】 ルータやレイヤ2-3スイッチのようなパケット中継装置において、従来からあるASICによるレイヤ2と3のルーティングおよび低レイヤのパケットのフィルタリングで中継することが決定されたパケットに対して、さらにASICやネットワークプロセッサによる高レイヤのフィルタリング機能をレイヤ毎やパケットの解析内容に応じて複数用意してパケット中継処理を行い、マルチレイヤでの高速パケット処理方法を提供する。



【特許請求の範囲】

【請求項1】パケット中継装置において、

レイヤ2およびレイヤ3のパケットを中継する第一の中継手段およびレイヤ2からレイヤ3または4までのレイヤの情報に基づきパケットの中継あるいは廃棄の判定をする第一のフィルタリング手段と、前記第一のフィルタリング手段で中継と決定されたパケットのレイヤ4または5からレイヤ7までのレイヤの任意の範囲の情報に基づきパケット中継あるいは廃棄の判定および中継するパケットの宛先を決定する第二のフィルタリング手段と、パケットを中継する第二の中継手段を備えることを特徴とするパケット中継装置。

【請求項2】請求項1に記載のパケット中継装置であって、

レイヤ2およびレイヤ3の経路制御プロトコルにより経路情報を収集し、ルーティングテーブルの作成および更新を行い、レイヤ2からレイヤ3または4までの情報に基づいてパケットのフィルタリングを行うための第一のフィルタリングテーブルと、レイヤ4または5からレイヤ7までの情報に基づいてパケットの宛先となる情報を決定する、またはフィルタリングを行うための第二のフィルタリングテーブルを作成するルーティング管理部と、

前記ルーティング管理部から配布された前記ルーティングテーブルの内容によりパケットの中継処理を行う第一のパケット中継処理部と、

前記ルーティング管理部から配布された前記第一のフィルタリングテーブルの内容によりパケットのフィルタリングを行う第一のフィルタリング処理部と、

前記第一のフィルタリング処理部により中継することが決定されたパケットについて前記ルーティング管理部から配布された前記第二のフィルタリングテーブルの内容により宛先となる情報を決定する、またはフィルタリングを行う第二のフィルタリング処理部と、

前記第二のフィルタリング処理部により中継することが決定され、それと同時に前記第二のフィルタリングテーブルの情報に基づいてパケットの変換を行い、パケットの中継を行う第二のパケット中継処理部とを、複数有するルーティング処理部が、内部通信線を介して複数接続されることを特徴とするパケット中継装置。

【請求項3】請求項1または2に記載のパケット中継装置であって、

サーバ装置群をエンドユーザからは仮想的に一つのサーバ装置として見えるようにする場合に、当該パケット中継装置が前記サーバ装置群の入口とした場合に、入力側となった前記ルーティング処理部で前記サーバ装置群に対してパケットを中継する手段を備えることを特徴とするパケット中継装置。

【請求項4】請求項1または2に記載のパケット中継装置であって、

サーバ装置群をエンドユーザからは仮想的に一つのサーバ装置として見えるようにする場合に、当該パケット中継装置が前記サーバ装置群の入口とした場合に、出力側となった前記ルーティング処理部で前記サーバ装置群に対してパケットを中継する手段を備えることを特徴とするパケット中継装置。

【請求項5】請求項1または2に記載のパケット中継装置であって、

前記パケット中継装置が宛先となるパケットに対して、前記ルーティング処理部が前記ルーティング管理部へのパケットであると判断した場合、前記ルーティング処理部内の前記第一のフィルタリング処理部または第二のフィルタリング処理部により、所定の前記パケットを廃棄する手段を備えることを特徴とするパケット中継装置。

【請求項6】請求項1または2に記載のパケット中継装置であって、

前記パケット中継装置が宛先となるパケットが、前記ルーティング処理部により前記ルーティング管理部へ中継された場合に、前記ルーティング管理部が前記第一のフィルタリング手段および前記第二のフィルタリング手段を有して、所定の前記パケットを廃棄する手段を備えることを特徴とするパケット中継装置。

【請求項7】請求項1または2に記載のパケット中継装置であって、

前記第一または第二のフィルタリングテーブルは、パケットのレイヤ毎のヘッダ情報またはインフォメーション部の情報を設定する条件フィールドと、その条件にマッチした場合に該当パケットを変換せずに中継する、変換して中継する、廃棄するか等を指示する第一の指示フィールドと、前記第一の指示フィールドで変換して中継すると指示された場合に、変換の方法を指示する第二の指示フィールドを有することを特徴とするパケット中継装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はパケット中継装置のマルチレイヤのパケット処理方法に関する。

【0002】

【従来の技術】従来の技術では、パケット中継装置であるルータやレイヤ2-3スイッチのパケット中継において、レイヤ4まではハードウェアでパケットのヘッダ情報等により中継やフィルタリングを行うことができる。レイヤ5以上になると、SSL (Secure Socket Layer) セッションIDやURL (Uniform Resource Locator) というような識別子のように想定可能なアプリケーションのパケットに対してはハードウェアでパケット処理をアシスト可能であるが、その他のパケットに対してはソフトウェアによりパケットを処理している。

【0003】従来の技術では、ハードウェアによるアシスト機能が限定され、ソフトウェアによる中継処理もC

PU処理性能によって上限が抑えられるという問題がある。

【0004】

【発明が解決しようとする課題】従来の技術では、すべてのレイヤでそのヘッダ情報等を見て高速にバケット中継やフィルタリングを実行するためには、ASIC (Application Specific Integrated Circuit) やネットワークプロセッサによるバケット処理が必要となるが、上位レイヤになるほどバケットのヘッダ部やインフォメーション部の情報量が増え、セッション数等の管理する情報も増える。そのため、ASICではある範囲の部分でしかアシストはできず、またネットワークプロセッサでも、プログラム規模が大きくなりネットワークプロセッサのプログラムメモリ内に入らないといった問題が発生する。

【0005】本発明の目的は、ルータやレイヤ2-3スイッチのようなバケット中継装置において、高レイヤのバケット処理を行う場合でも高速なバケット処理ができる方法を提供することにある。

【0006】

【課題を解決するための手段】本発明は、ルータやレイヤ2-3スイッチのようなバケット中継装置において、ASICによる低レイヤのバケットのフィルタリングの後、高レイヤのバケット処理を行うASICやネットワークプロセッサをレイヤ毎やバケットの解析範囲に応じて1つまたは複数用意して、マルチレイヤでの高速バケット処理方法を提供する。

【0007】

【発明の実施の形態】本発明の第一の実施の形態を図1から図10を参照して説明する。

【0008】図1は本実施形態を適用するバケット中継装置の構成例を示す図である。バケット中継装置100は、レイヤ2およびレイヤ3の経路制御プロトコルにより経路情報を収集し、ルーティングテーブルの作成および更新を行い、そしてネットワーク管理者によりバケットのフィルタリングの設定を行うルーティング管理部101と、ルーティング管理部101から配布されたルーティングテーブルやフィルタリングテーブルに基づき、バケットのルーティング処理を行う複数のルーティング処理部102 (102A、102Bないし102X) と、ルーティング管理部101と複数のルーティング処理部102を接続するスイッチ等の内部通信線103と回線インタフェース104を有する。

【0009】ルーティング管理部101は、CPU114、メインメモリ115、内部通信線116を介してバケットの送受信を制御するバケット制御部112を有する。またバケット制御部112に接続するバケットバッファ113を有する。バケット制御部112はスイッチアクセス制御部111により内部通信線103と接続される。

【0010】ルーティング処理部102は、CPU126、メインメモリ127、レイヤ2および3のルーティングとレイヤ2から4のフィルタリングを行うバケット制御部“L”122、レイヤ5から7のフィルタリングを行うバケット制御部“H”132を有しこれらが内部バス等の内部通信線128で接続されている。バケット制御部“L”122とバケット制御部“H”132は、ASICまたはネットワークプロセッサで構成することが望ましい。

10 【0011】バケット制御部“L”122は送受信されるバケットを格納するバケットバッファ“L”123を有し、バケット制御部“H”132は同様にバケットバッファ“H”133を有する。また、バケット制御部“L”122にはレイヤ2およびレイヤ3のルーティングテーブルやレイヤ2からレイヤ4のフィルタリングテーブルを格納するテーブルメモリ“L”125を有して送受信されるバケットのヘッダ等との比較を行うテーブル検索部“L”124が接続される。

20 【0012】同様にバケット制御部“H”132にはレイヤ5からレイヤ7のフィルタリングテーブルを格納するテーブルメモリ“H”134を有して送受信されるバケットのヘッダ等との比較を行うテーブル検索部“H”135が接続される。バケット制御部“L”122は1つまたは複数の回線インタフェース104を接続するポート制御部113と接続され、内部通信線103とスイッチアクセス制御部121を介して接続される。バケット制御部“H”132はバケット制御部“L”122と接続され、内部通信線103とスイッチアクセス制御部121を介して接続される。尚、他のルーティング処理部102Bないし102Xも同様の構成を有する。

30 【0013】図1のバケット中継装置の構成例は、バケットのレイヤ2から7までの情報をバケット制御部を2つ用意して、1つめのバケット制御部“L”122でレイヤ2からレイヤ4までのフィルタリングを行い、2つめのバケット制御部“H”132でレイヤ5から7のフィルタリングを行う例を示しているが、この例に限定されず、バケット制御部をレイヤ毎やバケットの解析内容に応じて複数用意することも可能である。

40 【0014】以下では、まずWEB等のサーバへの一般的なアクセスの方法や、レイヤ4-7スイッチを用いた場合のアクセスの方法を説明し、その次に本実施形態を適用するバケット中継装置を使用した場合のネットワーク構成の一例および処理概要について説明する。

50 【0015】図2はインターネットでWEBサーバをアクセスする際に利用されるHTTP (Hyper Text Transport Protocol) のバケットの例を示す図である。HTTPメッセージ210は、リクエストやレスポンス等の情報を示すHTTPヘッダ211と、HTTPボディ212から構成される。LAN環境でHTTPメッセージ210は、MAC (Media Access Control) ヘッダ22

1と、IP (Internet Protocol) ヘッダ222と、TCP (Transmission Control Protocol) ヘッダ223を付加されたHTTPパケット220として構成される。

【0016】また、セキュリティを考慮してSSL (Secure Socket Layer) を使用した場合、HTTPメッセージ210は暗号化されたHTTPメッセージ235となり、SSLヘッダ234が付加されたHTTPパケット230として構成される。それぞれのデータの概要については、MACヘッダ221のTYPEフィールドが0x0800 (16進数) の場合はその上位のプロトコルがIPであることを示し、IPヘッダ222のPROTOCOLフィールドが6の場合はその上位のプロトコルがTCPであることを示し、TCPヘッダ223の宛先ポート番号が80である場合はその上位のプロトコルがHTTPであることを示し、またTCPヘッダ223の宛先ポート番号が443である場合はその上位のプロトコルがSSLを利用したHTTPであることを示している。

【0017】図3はクライアントがインターネットやLANのようなネットワークを介して、WEBサーバやFTP (File Transfer Protocol) サーバを利用する場合のネットワーク構成の一例を示す図である。端末301AがWEBサーバ302Aをアクセスする場合、まずネットワーク300内のDNS (Domain Name Server) 304とのメッセージのやりとり305Aにより、WEBサーバ302Aのホスト名からIPアドレスを取得し、このIPアドレスを宛先とするHTTPのリクエストメッセージ306AがWEBサーバ302Aに送信される。WEBサーバ302Aは、HTTPのリクエストメッセージ306Aのリクエスト内容に応じたHTTPのレスポンスメッセージ307Aを端末301Aに送信する。

【0018】HTTPのレスポンスメッセージ307Aの宛先アドレスはリクエストメッセージ306Aの送信元IPアドレスが用いられるため、DNS304は使用されない。DNS304はホスト名とIPアドレスの対応を管理しており、このネットワーク構成の例では一しか示していないが、ドメインが複数存在する場合にはドメインを管理する範囲に応じて複数存在することもあり、複数のDNS間で連携してホスト名とIPアドレスの対応を管理する。端末301BがWEBサーバ302Cをアクセスする場合、端末301CがFTPサーバ303Bをアクセスする場合も、前記と同様なメッセージのやりとりが行われる。ただし、FTPサーバ303をアクセスする場合には、HTTPメッセージを用いる場合と、FTPプロトコルを利用する場合がある。

【0019】図4はクライアントがインターネットやLANのようなネットワークを介して、WEBサーバやFTPサーバを利用する際に、レイヤ4-7スイッチを用いている場合のネットワーク構成の一例を示す図であ

る。WEBサーバ402Aないし402Cはレイヤ4-7スイッチ406Aにより仮想ホスト名402Gとして管理され、FTPサーバ403Aないし403Cはレイヤ4-7スイッチ406Bにより仮想ホスト名403Gとして管理されているものとし、クライアントが仮想ホスト名でサーバをアクセスするために、レイヤ4-7スイッチ406とDNS304は情報の交換を行っているものとする。

【0020】端末401AがWEBサーバ402Gをアクセスする場合、図3での説明と同様にDNS304とのやりとりの後、HTTPのリクエストメッセージ407AがWEBサーバ402Gに送信される。その際、レイヤ4-7スイッチ406AがHTTPのリクエストメッセージ407Aの内容やWEBサーバ402Aないし402Cの稼動状況により、適切なWEBサーバへとHTTPのリクエストメッセージを振り分ける。この例では、HTTPのリクエストメッセージ407Aは、408AとしてWEBサーバ402Aに送信されるものとしている。

【0021】HTTPのリクエストメッセージ407Aは、図2で示したようにSSLを使用している場合は、暗号化された内容をレイヤ4-7スイッチ406Aが暗号をデコードしてHTTPのリクエストメッセージ408Aでは復号化する場合もある。WEBサーバ402Aは、HTTPのレスポンスメッセージ409Aを端末401Aを送信する。その際に前記のように、レイヤ4-7スイッチ406Aが暗号化されていないHTTPのレスポンスメッセージ409Aを暗号化してHTTPのレスポンスメッセージ410Aとして送信する場合もある。端末401BがWEBサーバ402Gをアクセスする場合、端末401CがFTPサーバ403Gをアクセスする場合も、前記と同様なメッセージのやりとりが行われる。ただし、サーバ側からクライアント側へのメッセージは、409Bや409Cのようにレイヤ4-7スイッチ406Aや406Bを介さない場合もある。

【0022】図5は本実施形態を適用するパケット中継装置100を用いたネットワーク構成の一例を示す図である。パケット中継装置100、端末501、WEBサーバ502、FTPサーバ503、DNS304が、ネットワーク610ないし670を介して接続される。パケット中継装置100は、レイヤ2およびレイヤ3のルーティング処理を行い、かつ、図4で示したレイヤ4-7スイッチ406と同様に適切なWEBサーバやFTPサーバへとHTTPのメッセージを振り分ける。レイヤ4-7スイッチとの違いは、同一のネットワーク上にないWEBサーバ502Aないし502Cをパケット中継装置100Aにより仮想ホスト名502Gでアクセスできるようにすることや、FTPサーバ503Aないし503Cをパケット中継装置100Bにより仮想ホスト名503Gでアクセスできるようにすることである。

【0023】図6は図5で示されるネットワークやパケット中継装置、端末等に割り当てられているIPアドレスの一例を示す図である。図7(a)はパケット中継装置100Aのテーブルメモリ“L”125に格納されるルーティングテーブル700Aの一例を示す図であり、図7(b)は中継装置100Bのテーブルメモリ“L”125に格納されるルーティングテーブル700Bの一例を示す図である。ルーティングテーブル700は、ネットワークアドレス701、ネクストホップアドレス702、および出力ポート703を一組とするエントリ704を複数格納する構成となっている。

【0024】図8はパケット中継装置100のテーブルメモリ“L”125に格納されるフィルタリングテーブル“L”800の一例を示す図である。フィルタリングテーブル“L”800は、レイヤ2から4までのマッチ条件801、マッチしたときの処理802、およびパケット制御部“H”132に転送したときに使用する処理ID803を一組とするエントリを複数格納する(804、805、806等)構成となっている。図9はパケット中継装置100のテーブルメモリ“H”134に格納されるフィルタリングテーブル“H”900の一例を示す図である。フィルタリングテーブル“H”900は、図8で示した処理ID803をキーとして検索するための処理ID901、レイヤ5から7までのマッチ条件902、およびマッチしたときの処理903を一組とするエントリを複数格納する(904、905、906等)構成となっている。

【0025】図10はルーティング処理部102がパケットを受信してからパケットを内部通信線103、またはポート制御部113へパケットを送信するまでの処理手順の一例を示す図である。図5において、端末501Aおよび501BがWEBサーバ502Gをアクセスする場合、パケット中継装置100Aは端末501Aからのパケットを受信すると(ステップ1011)、まずパケット処理“L”1010を行う。パケット処理“L”1010においては、パケット受信(ステップ1012)と同時にパケットのレイヤ2、3、4のヘッダ解析を行い(ステップ1013)、ルーティングテーブル700Aの検索を行う(ステップ1014)。

【0026】受信したパケットの宛先アドレスは192.168.30.30であるので、エントリ705がマッチして、ネットワークアドレスは192.168.30.0、ネクストホップアドレスは192.168.30.1、出力ポートはPA2であることがわかる。さらに、フィルタリングテーブル“L”800の検索を行い、エントリ804がマッチして、パケット制御部“H”へ転送することになり、転送パケットの作成を行い(ステップ1015)、処理ID803が「001」であるという情報を渡して、パケット処理“H”1020を行う。

【0027】その他の受信パケットについては、ルーテ

ィングテーブル700に宛先がない場合や、フィルタリングテーブル800で条件がマッチして廃棄となっている場合は、そのパケットは廃棄される(ステップ1015)。ルーティングテーブル700に宛先が存在して、フィルタリングテーブル800にマッチする条件がない場合は、そのパケットはパケット送信処理を行う(ステップ1030)。レイヤ2、3、4のヘッダ解析を行って(ステップ1013)、IPヘッダやTCPヘッダにオプションヘッダが設定されている場合等は、ソフトウェア処理を行う(ステップ1040)。

【0028】パケット処理“H”1020においては、パケット受信(ステップ1021)と同時にパケットのレイヤ5以上のヘッダ解析を行い(ステップ1022)、フィルタリングテーブル“H”900の検索を行う(ステップ1023)。パケット処理“L”1010から渡された処理IDを元に、フィルタリングテーブル“H”900の処理ID901が「001」の中から、エントリ904がマッチした場合、IPヘッダのDAを192.168.30.10に設定することになり、再度ルーティングテーブル700Aの検索を行い、ネクストホップアドレスと出力ポートは変化せずに、転送パケットの作成を行い(ステップ1024)、パケット送信処理を行う(ステップ1030)。この時の端末501AからWEBサーバ502Gへのパケットの流れは、図5の504Aようになる。前記ステップ1023において、受信したパケットは端末501Bからのものとして、フィルタリングテーブル“H”900の処理ID901が「001」の中から、エントリ905がマッチした場合、IPヘッダのDAを192.168.40.10に設定することになり、再度ルーティングテーブル700Aの検索を行い、ネクストホップアドレスと出力ポートは、エントリ706のように変化して、転送パケットの作成を行い(ステップ1024)、パケット送信処理を行う(ステップ1030)。

【0029】この時の端末501BからWEBサーバ502Gへのパケットの流れは、図5の504Bようになる。端末501CがFTPサーバ503Gをアクセスする場合、パケット中継装置100は前記と同様の処理を行う。この場合、フィルタリングテーブル“L”800ではエントリ806がマッチし、フィルタリングテーブル“H”ではエントリ906がマッチして、レイヤ5以上の内容については不問で、FTPサーバ503Gの実際のFTPサーバ503Aないし503Cの中で、この時点で負荷の一番低いFTPサーバ503Bのアドレス192.168.50.10をIPヘッダのDAに設定し、再度ルーティングテーブル700Aの検索を行い、ネクストホップアドレスと出力ポートは変化せずに、転送パケットの作成を行い(ステップ1024)、パケット転送処理を行う(ステップ1030)。この時の端末501CからFTPサーバ503Gへのパケットの流れは、図5の

504Cようになる。

【0030】第一の実施の形態では、バケット中継装置がレイヤ4-7の情報をもとにサーバをアクセスする場合のサーバ選択の一例を示したが、バケット制御部

“L”122でレイヤ2から4のバケット処理、バケット制御部“H”132でレイヤ5から7のバケット処置を行うような様々な例、例えばファイアウォール機能やQoS (Quality of Service) 機能を実現する際にも使用できる。

【0031】次に本発明の第二の実施形態を図11と図12を参照して説明する。第二の実施形態では、第一の実施形態で説明したバケット制御部“H”132の処理を入力側のルーティング処理部132で行う場合と、出力側のルーティング処理部132で行う場合の処理概要について説明する。

【0032】図11はバケット中継装置100において、ネットワーク1101Aからサーバ1102Aないし1102Cをアクセスする場合に、入力側のルーティング処理部102Aのバケット制御部“H”132Aで、第一の実施の形態で説明したようなサーバの選択が行われた場合のバケットの流れを示す図である。

【0033】通常は1103のようなバケットの流れであるとして、バケット制御部“H”132Aがレイヤ5以上の情報により、サーバ1102Aないし1102Cを選択するような処理の場合、バケットの流れは途中までは1104で、バケット制御部“H”132Aからは1105Aないし1105Cようになる。この場合の出力側のルーティング処理部はどれでも選択できる可能性があるため、サーバ群を広域に配置するのに適しているが、入力側のバケット制御部“H”132Aの処理負荷が大きくなる可能性がある。

【0034】図12はバケット中継装置100において、ネットワーク1201Aからサーバ1202Aないし1202Cをアクセスする場合に、出力側のルーティング処理部132Bのバケット制御部“H”132Bで、第一の実施の形態で説明したようなサーバの選択が行われた場合のバケットの流れを示す図である。通常は1203のようなバケットの流れであるとして、バケット制御部“H”132Bがレイヤ5以上の情報により、サーバ1202Aないし1202Cを選択するような処理の場合、バケットの流れは途中までは1204で、バケット制御部“H”132Bからは1205Aないし1205Cようになる。この場合の出力側のルーティング処理部は一つしか選択できない可能性があるため、サーバ群をルーティング処理部の配下に配置するのに適している。バケット制御部“L”122Aによりレイヤ2から4の情報で、出力側のルーティング処理部102を複数選択できる場合は、図12のルーティング処理部102Bのバケットの流れが他のルーティング処理部でも実施されるような形態となる。

【0035】次に本発明の第三の実施の形態を図13と図14を参照して説明する。第三の実施の形態では、第一の実施の形態で説明したバケット制御部の処理で、バケットの宛先がルーティング管理部宛となった場合として、DoS攻撃やDDoS (DDoS=Distributed Denial of Service) 攻撃のような悪意のあるバケットを、ルーティング処理部内のバケット制御部で廃棄する場合と、ルーティング管理部内にバケット制御部“H”を有することにより廃棄する場合の処理概要について説明する。

【0036】図13と図14はバケット中継装置100のルーティング管理部101を宛先とするバケットを受信した場合のバケット中継装置100の構成の一例とバケットの流れを示す図である。ルーティング管理部101宛のバケットには、経路制御プロトコルなどの制御バケットがほとんどであるが、場合によってはバケット中継装置の動作に問題を生じさせるようなバケットである可能性もある。このようなバケットを、図13ではバケット制御部“L”122Aとバケット制御部“H”132Aで、図14ではバケット制御部122Aとルーティング管理部101にレイヤ5から7までのフィルタリングを行うバケット制御部“H”1401を有することで、廃棄できるようにする。

【0037】DoS攻撃の代表的なものとしては、要求されていないPing応答メッセージやIPアドレスが不正なメッセージの大量送信等があるが、これらはバケット制御部“L”122のフィルタリングテーブル800で廃棄指定が可能である。つまり、レイヤ2から4までの情報により不正なバケットやDoS攻撃のバケットはフィルタリングテーブル800の廃棄指定により廃棄できる。

【0038】しかし、この廃棄指定だけではフィルタリングできないバケット、すなわちレイヤ2から4までの情報だけでは正常なバケットと見える悪意のあるバケットを図13ではバケット制御部“H”132、図14ではバケット制御部“H”1401のフィルタリングテーブル900の廃棄指定で廃棄できるようにする。これにより、例えば、HTTPでWEBサーバに存在しないページのリクエストを大量送信して、Not Foundのレスポンスメッセージを大量発生させるようなバケットを廃棄できるようになる。

【0039】また、上記実施形態の応用により、ルータ、レイヤ2-3スイッチ、アプリケーションスイッチ、コンテンツ内容によるスイッチングやロードバランス等、を実現することができる。

【0040】

【発明の効果】本発明によれば、マルチレイヤでの高速バケット処理を実現できる。

【図面の簡単な説明】

【図1】バケット中継装置の構成例を示す図。

11

【図2】HTTPパケットの構成例を示す図。

【図3】サーバをアクセスする例を示す図。

【図4】レイヤ4-7スイッチを使用し、サーバをアクセスする例を示す図。

【図5】パケット中継装置を使用し、サーバをアクセスする例を示す図。

【図6】ネットワークと装置のIPアドレスの例を示す図

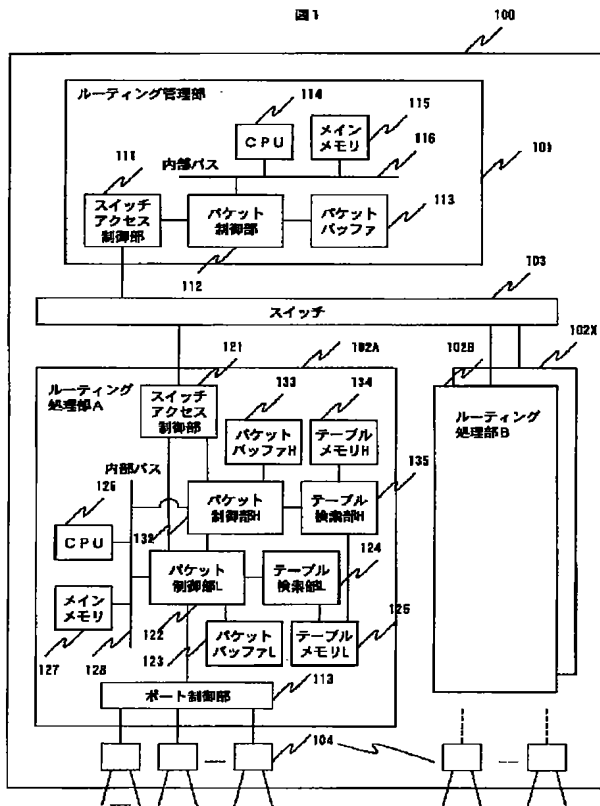
【図7】ルーティングテーブルの構成例を示す図。

【図8】フィルタリングテーブル“L”の構成例を示す図。

【図9】フィルタリングテーブル“H”の構成例を示す図。

【図10】パケット送受信処理の処理概要を示す図。 *

【図1】



12

* 【図11】入力側のパケット制御部でサーバ選択を行う例を示す図。

【図12】出力側のパケット制御部でサーバ選択を行う例を示す図。

【図13】ルーティング管理部宛のパケットをルーティング処理部内のパケット制御部で廃棄する例を示す図。

【図14】ルーティング管理部宛のパケットをルーティング管理部内のパケット制御部で廃棄する例を示す図。

【符号の説明】

100…パケット中継装置

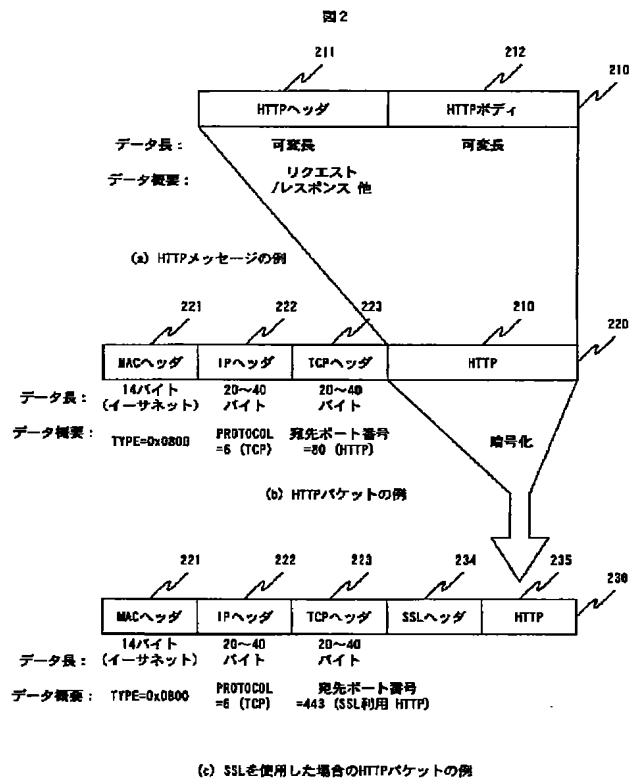
112、122、132、1401…パケット制御部

220、230…HTTPパケット

800…フィルタリングテーブル“L”

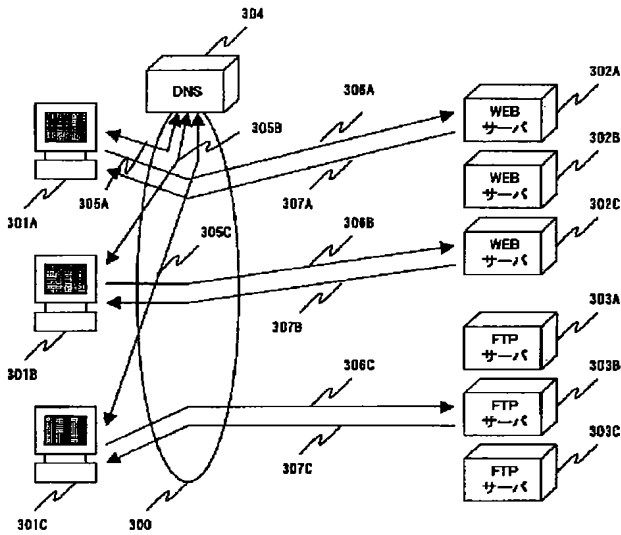
900…フィルタリングテーブル“H”

【図2】



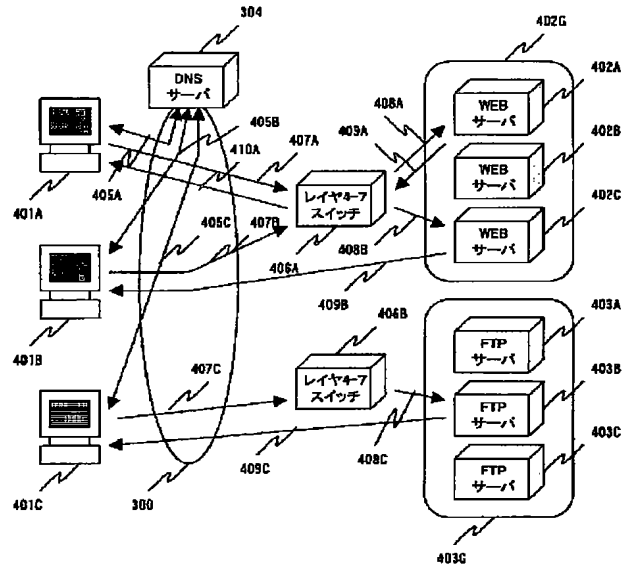
【図3】

図3



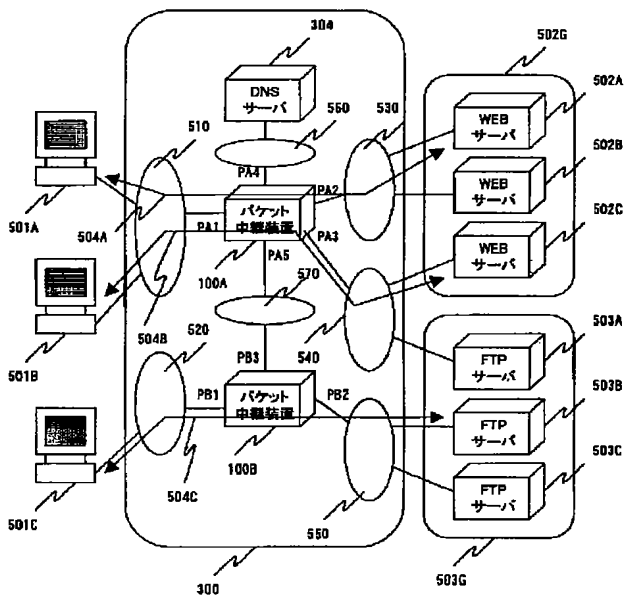
【図4】

図4



【図5】

図5



【図8】

図8

801	802	803	804
マッチ条件	処理	処理ID	
(IPヘッダのDA = 192.168.30.30) AND (TCPヘッダの宛先ポート = 80 (HTTP))	パケット制御部Hへ転送	001	805
IPヘッダのSA = 192.168.30.10	廃棄		806
...	...		
(IPヘッダのDA = 192.168.50.50) AND (TCPヘッダの宛先ポート = 21 (FTP))	パケット制御部Hへ転送	002	
...	...		

【図9】

図9

901	902	903	904
処理ID	マッチ条件	処理	
001	URL = www.502.net/index1.htm	IPヘッダのDAを192.168.30.10に設定	905
001	URL = www.502.net/index3.htm	IPヘッダのDAを192.168.40.10に設定	906
...	
002	すべてマッチ	IPヘッダのDAを最も低いFTPサーバのIPアドレスに設定	
...	

【図6】

図6 (a)

ネットワーク/装置	IPアドレス
ネットワーク510	192.168.10.0
ネットワーク520	192.168.20.0
ネットワーク530	192.168.30.0
ネットワーク540	192.168.40.0
ネットワーク550	192.168.50.0
ネットワーク560	192.168.60.0
ネットワーク570	192.168.70.0
パケット中継装置100A ポートPA1	192.168.10.1
パケット中継装置100A ポートPA2	192.168.30.1
パケット中継装置100A ポートPA3	192.168.40.1
パケット中継装置100A ポートPA4	192.168.60.1
パケット中継装置100A ポートPA5	192.168.70.1
パケット中継装置100B ポートPB1	192.168.20.1
パケット中継装置100B ポートPB2	192.168.50.1
パケット中継装置100B ポートPB3	192.168.70.2

図6 (b)

ネットワーク/装置	IPアドレス
端末501A	192.168.10.10
端末501B	192.168.10.20
端末501C	192.168.20.10
DNS504	192.168.60.10
WEBサーバ502A	192.168.30.10
WEBサーバ502B	192.168.30.20
WEBサーバ502C	192.168.40.10
WEBサーバ502G	192.168.30.30
WEBサーバ503A	192.168.40.20
WEBサーバ503B	192.168.50.10
WEBサーバ503C	192.168.50.20
WEBサーバ503G	192.168.50.30

【図7】

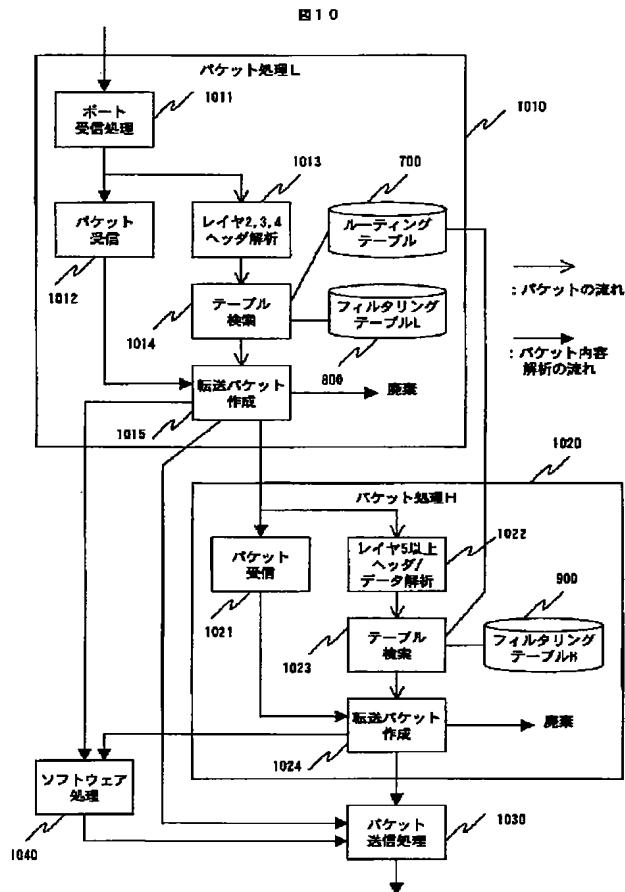
図7 (a)

ネットワーク	ネクストホップ	出力ポート
192.168.10.0	192.168.10.1	PA1
192.168.20.0	192.168.70.2	PA5
192.168.30.0	192.168.30.1	PA2
192.168.40.0	192.168.40.1	PA3
192.168.50.0	192.168.70.2	PA5
192.168.60.0	192.168.60.1	PA4
192.168.70.0	192.168.70.1	PA5
...

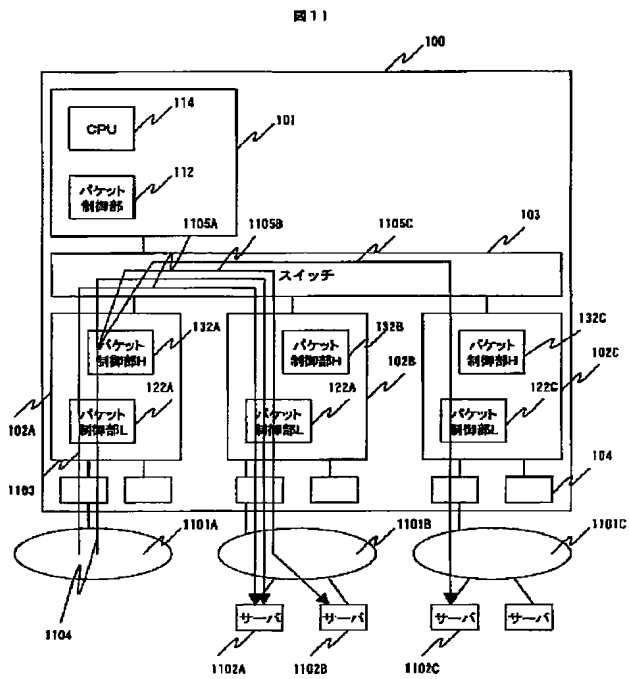
図7 (b)

ネットワーク	ネクストホップ	出力ポート
192.168.10.0	192.168.70.1	PB3
192.168.20.0	192.168.20.1	PB1
192.168.30.0	192.168.70.1	PB3
192.168.40.0	192.168.70.1	PB3
192.168.50.0	192.168.50.1	PB2
192.168.60.0	192.168.70.1	PB3
192.168.70.0	192.168.70.2	PB3
...

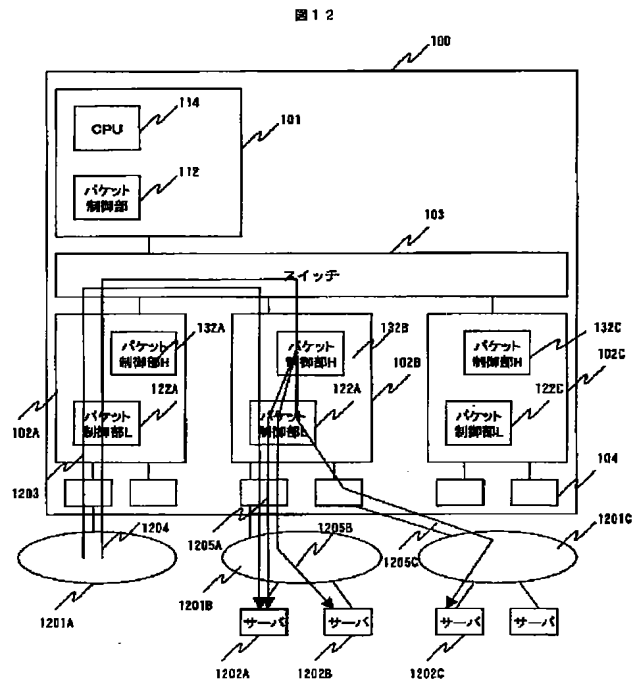
【図10】



【図11】

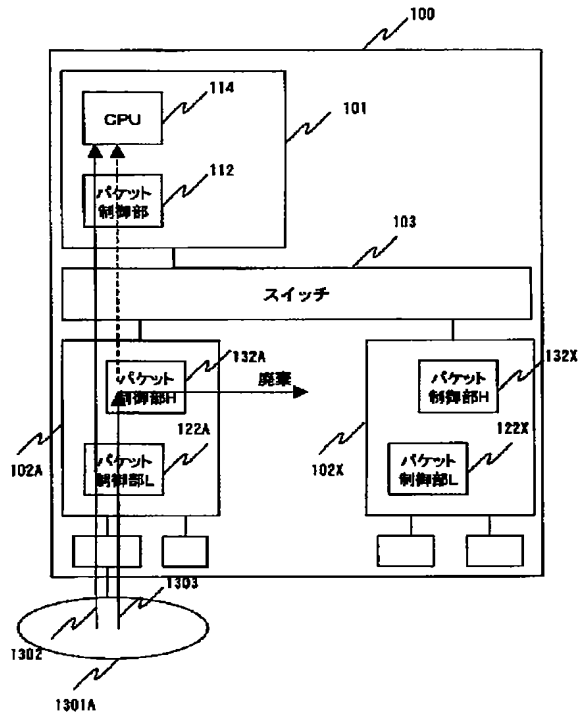


【図12】



【図13】

図13



【図14】

図14

